

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets

(11)



EP 1 073 294 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:

31.01.2001 Bulletin 2001/05

(51) Int Cl. 7: H04Q 7/24

(21) Application number: 00306447.4

(22) Date of filing: 28.07.2000

(84) Designated Contracting States:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE

Designated Extension States:

AL LT LV MK RO SI

(30) Priority: 30.07.1999 GB 9918046

(71) Applicant: Nokia Networks Oy

02150 Espoo (FI)

(72) Inventors:

- Numminen, Raili
33610 Tampere (FI)
- Närvenen, Kai
33960 Pirkkala (FI)
- Rantala, Tero
33680 Tampere (FI)

(74) Representative: Slingsby, Philip Roy et al

Page White & Farrer

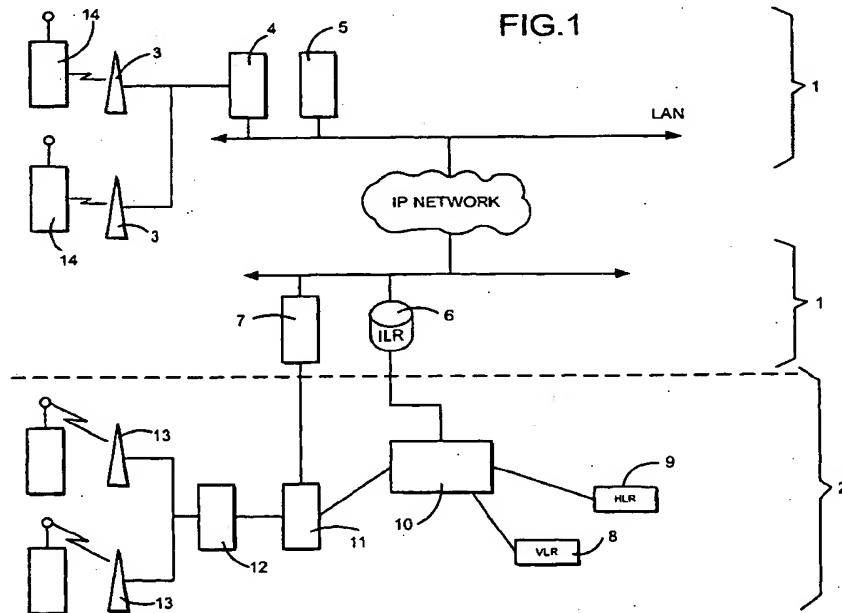
54 Doughty Street

London WC1N 2LS (GB)

(54) Network access control

(57) An access control system for controlling access by wireless terminals to a wireless telecommunications network, the access control system comprising: a database storing the identities of a set of wireless terminals belonging to the telecommunications network; a configurable store for storing a supplementary access value indicative of whether terminals that do not belong to the telecommunications network may access the network;

and an access control unit for receiving an access request message indicating the identity of a wireless terminal and in response to that message accessing the database and/or the store to permit access by the wireless terminal to the wireless telecommunications network if: a. the identity of the wireless terminal is present in the database; or b. the supplementary access value indicates that terminals that do not belong to the telecommunications network may access the network.



Description**Field of the Invention**

[0001] The present invention relates to a company intranet and in particular to a method for dealing with visitors.

Background of the Invention

[0002] Prior art office-based communications systems usually operate conventional fixed-line telephone units linked via an internal switchboard or PBX (private branch exchange.) Such fixed-line systems are able to provide relatively high voice quality. However, user mobility is severely impaired. It is also known to connect a base unit for a cordless system such as DECT to the internal PBX. This allows users to use cordless handsets in the office, but the server handsets (unless they are equipped with a dual-mode capability) can not be used outside the local cordless coverage area.

[0003] The improvement of digital cellular telephone technologies means that cellular telephone systems can now provide equivalent, if not higher, voice quality than fixed-line systems. Mobile systems also allow greater freedom of movement for the user within the office than do fixed-line systems. However, there can often be difficulties in receiving cellular telephone signals in an office.

[0004] RCP (Rich Call Platform) is a proprietary communications system developed by the applicants which introduces the concept of utilising mobile telephone units, such as conventional GSM mobile stations, in an office environment. The system preferably makes use of a known concept called Internet Telephony or Voice-over-IP (Internet Protocol).

[0005] Voice-over-IP is a technology which allows sound information to be transmitted over existing IP-based Local or Wide Area Networks or the Internet. In a similar way, data and video information can be encoded so as to be capable of transmission over the same networks. The technology thus provides for convergence and integration of three different media types over the same network.

[0006] Prior to the advent of Voice-over-IP, offices often operated three separate networks for the transmission of these media types. As indicated above, fixed-line telephone systems coupled to an in-house PBX provided for voice communication, an office-based LAN or Intranet (i.e. a packet-switched internal network), normally comprising computer terminals linked via network cards and under the control of a server station, provided for the transmission of "conventional" computer data, and video cameras linked to monitors via fixed line or remote transmission link provided for video communication.

[0007] Voice-over-IP effectively combines these three media types such that they can be transmitted simultaneously on the same packet-switched intranet network

or IP-routed throughout the office environment and, using an external network such as the internet, beyond the confines of the office.

[0008] In order to provide for such media convergence, Voice-over-IP often uses a specific ITU (International Telecommunication Union) standard protocol to control the media flow over the Intranet. One common standard protocol used in Voice-over-IP systems, and the one used in the RCP system, is termed H.323.

[0009] H.323 is an ITU standard for multimedia communications (voice, video and data) and allows multimedia streaming over conventional packet-switched networks. The protocol provides for call control, multimedia management and bandwidth management for both point-to-point (2 end-users) and multipoint (3 or more end-users) conferences. H.323 also supports standard video and audio codecs (compression/decompression methods such as MPEG) and supports data sharing via the T.120 standard.

[0010] Furthermore, H.323 is network, platform and application independent allowing any H.323 compliant terminal to operate in conjunction with any other terminal.

[0011] The H.323 standard defines the use of three further command and control protocols:

- a) H.245 for call control;
- b) Q.931 for call signalling; and
- c) The RAS (Registrations, Admissions and Status) signalling function.

[0012] The H.245 control channel is responsible for control messages governing the operation of the H.323 terminal including capability exchanges, commands and indications. Q.931 is used to set up a connection between two terminals. RAS governs registration, admission and bandwidth functions between endpoints and Mobile Telephone Server (defined later).

[0013] For an H.323 based communication system, the standard defines four major components:

- 1. Terminal
- 2. Gateway
- 3. Mobile Telephone Server
- 4. Multipoint Control Unit (MCU)

[0014] Terminals are the user end-points on the network, e.g. a telephone or fax unit or a computer terminal. All H.323 compliant terminals must support voice communications, but video and data support is optional.

[0015] Gateways connect H.323 networks to other networks or protocols. For an entirely internal communications network i.e. with no external call facility, gate-

ways are not required.

[0016] Mobile Telephone Servers are the control centre of the Voice-over-IP network. It is under the control of a Mobile Telephone Server that most transactions (communication between two terminals) are established. Primary functions of the Mobile Telephone Server are address translation, bandwidth management and call control to limit the number of simultaneous H.323 connections and the total bandwidth used by those connections. An H.323 "zone" is defined as the collection of all terminals, gateways and multipoint-control units (MCU - defined below) which are managed by a single Mobile Telephone Server.

[0017] Multipoint Control Units (MCU) support communications between three or more terminals. The MCU comprises a multipoint controller (MC) which performs H.245 negotiations between all terminals to determine common audio and video processing capabilities, and a multipoint processor (MP) which routes audio, video and data streams between terminals.

[0018] The conventional Voice-over-IP system described herein above normally utilises standard fixed-line telephone systems which are subject to the disadvantages outlined above, namely the lack of mobility and the lack of user commands.

[0019] The RCP concept takes Voice-over-IP further in that it provides for the use of conventional mobile telephone units, such as GSM mobile stations, within the Voice-over-IP system. To provide for such mobile communications within an intra-office communication network, RCP combines known Voice-over-IP, as described above, with conventional GSM-based mobile systems.

[0020] GSM base stations are provided to give coverage within the office, and are connected to the company's intranet. Intra-office calls to or from cellular telephones in the office are routed through the office intranet and extra-office calls are routed conventionally through the GSM network. Such a system provides most or all of the features supported by the mobile station and the network such as telephone directories, short messaging, multiparty services, data calls, call barring, call forwarding etc. RCP, therefore, provides for integrated voice, video and data communications by interfacing an H.323-based voice-over-IP network with a GSM mobile network.

[0021] The RCP system is a cellular network, similar to the conventional GSM network and is divided into H.323 Zones as described above. One H.323 Zone may comprise a number of cells. Two or more H.323 zones may be contained within an administrative domain. The allocation of H.323 zones to an administrative domain is an issue primarily concerning billing and is therefore not relevant to this invention.

[0022] A company RCP may be physically located in two or more separate office sites. These sites may reside in two different countries in areas managed by two or more different GSM operators. They may also reside

in different regions of a country, in which two different GSM operators would be competing for customers.

[0023] It would be desirable to provide a method of allowing subscribers to use the internal site network when visiting different sites belonging to the same company and to make calls from their own site to other company sites which are routed over the company RCP system, and without being routed outside the company's own network.

[0024] It would be desirable to have a method for controlling access to the RCP network (or another like network), that would be configurable to allow or disallow visitors to use the network for signalling and calls outside the RCP system at any particular time.

Statement of the Invention

[0025] According to one aspect of the present invention, there is provided an access control system for controlling access by wireless terminals to a wireless telecommunications network, the access control system comprising:

a database storing the identities of a set of wireless terminals belonging to the telecommunications network; a configurable store for storing a supplementary access value indicative of whether terminals that do not belong to the telecommunications network may access the network; and an access control unit for receiving an access request message indicating the identity of a wireless terminal and in response to that message accessing the database and/or the store to permit access to the wireless telecommunications network by the wireless terminal if:

a. the identity of the wireless terminal is present in the database; or
b. the supplementary access value indicates that terminals that do not belong to the telecommunications network may access the network.

[0026] According to a second aspect of the present invention there is provided a method for controlling access by wireless terminals to a wireless telecommunications network having a database storing the identities of a set of wireless terminals belonging to the telecommunications network and a configurable store for storing a supplementary access value indicative of whether terminals that do not belong to the telecommunications network may access the network, the method comprising:

receiving an access request message indicating the identity of a wireless terminal; accessing the database to determine whether the identity of the wireless terminal is present in the database and/or accessing the supplementary access value to determine whether it indicates that terminals that do not belong to the telecommunications network may access the network; and if:

a. the identity of the wireless terminal is present in the database; or

b. the supplementary access value indicates that terminals that do not belong to the telecommunications network may access the network; transmitting a message to permit the wireless terminal access to the wireless telecommunications network.

[0027] The access control unit may suitably be configured to permit or deny access to the network by means of transmitting a permission or denial message. That message may, for example, be transmitted to the terminal itself or to another network. That other network may be a network which the terminal currently is permitted to access.

[0028] The access request message may be a location update request. The access control unit suitably replies to such a location update request by transmitting a location update response. Where access is to be denied the message may be a location update reject message, preferably (where this is provided for) with a value indicative of location access not being allowed.

[0029] If:

- a. the identity of the wireless terminal is not present in the database; and
- b. the supplementary access value indicates that terminals that do not belong to the telecommunications network may not access the said network; then the access control unit suitably denies access by the terminal to the network.

[0030] One or other or both of the networks may be operable according to the GSM standard or a derivative thereof. The said network is suitably a localised network, preferably one employing an intranet or other packet-based communications system for at least some traffic communications. The said network is suitably under the control of an operator of the other network. One or both of the networks may be cellular telephone systems. The said identities may be provided as any suitable identifier. In a GSM system, or in certain other systems derived from the GSM standard, the identities may be IMSIs. In other networks the equivalent level of identification is preferably used.

[0031] The wireless telecommunications network could be a data network.

[0032] The access control unit need not be the only unit that has control over access to the said network. The access control unit could itself be under the control of another unit (e.g. a unit at the other network) or could share control with such a unit.

Brief Description of the Drawings

[0033] The present invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 shows schematically components of the in-

tranet and external internet and mobile telecommunications system which are related to the present invention.

Figure 2 is a flowchart indicating the method of operation of the system.

Description Of The Preferred Embodiment

[0034] Figure 1 shows schematically some components of an office intranet and an external internet and mobile telecommunications system. The office intranet area is indicated generally by 1 and the external internet and mobile telecommunications system area is indicated generally by 2.

[0035] The relevant components of the intranet system 1 as shown are a Base Transceiver Station (BTS) 3, an Intranet Mobile Cluster (IMC) 4, a RCP Mobile Telephone Server (MTS) 5, an Intranet Location Register (ILR) database 6 and an A-Intranet Gateway 7. These components are connected over a wireless Local Area Network (LAN), forming the "office network" 1.

[0036] The relevant components of the internet and mobile telecommunications system 2 as shown are a Visitor Location Register (VLR) 8, an integrated Home Location Register, Authentication Centre and Equipment Identity Register (HLR/AC/EIR) 9, a Mobile Switching Centre (MSC) 10, a Transcoder and Subrate Channel Multiplexer (TSCM) 11, a Base Station Controller (BSC) 12 and BTSs 13. Together these components form the "operator network" 2. The VLR and the HLR and other registers could be integrated as part of the MSC. In this example the wireless telephone service is a GSM service, but the service could be provided by other communications systems.

[0037] The BTS 3 is equivalent to the BTSs 13 in the GSM operator network and its purpose is to receive and transmit signals to and from mobile phones and to interface with the IMC. The IMC is equivalent to a Base Station Controller in a standard GSM network. Its functions include detection of the possible need for handover, generation of speech and data frames, configuration of the BTS, control of interfacing with the MTS including status enquiry and establishing calls to/from the BTS. The MTS is responsible for controlling access to the intranet, by using information obtained from the ILR, as will be described in more detail below. The ILR is managed by the home GSM network operator and resides in the home GSM operator premises. It has access to two GSM registers via a MAP interface, namely the HLR 9 and VLR 8. The HLR and VLR hold all the location information of all subscribers. The HLR is a database which contains all the data concerning the access capabilities of subscribers of the site with which it is associated, and services to which they are entitled. Also the HLR provides MSCs associated with other sites with similar information to allow the subscriber to receive calls whilst visiting another site which is part of the same intranet. The Equipment Identity Register within an Au-

45

50

55

thentication Centre allows interrogation of the HLR for verifying whether a user is listed in the HLR. The VLR stores subscriber information for all mobile phones which enter its area of coverage, which allows the MSC to set up calls to and from such phones. When a mobile phone enters its area, the subscriber data is interrogated and can be added to the VLR, so the VLR would contain the address of the subscriber's HLR.

[0038] The office and operator networks 1,2 are connected by three interfaces :

A-interface at the Intranet Gateway 7 of office network 1 to the TCSM 11 - this is a GSM-specified gateway which controls operation, maintenance and transcoder functions and is the route used for speech. The TCSM is a further interface which interfaces with the MSC 10.

Pulse Code Modulation (PCM) providing a physical connection between the ILR 6 and the MSC 10 - for data and signalling

Mobile Application Part (MAP) interface protocol between the ILR 6 and the MSC 10 - for data and signalling

[0039] In a typical office environment having an internal intranet, company members and a variable number of visitors, all carrying GSM mobile phones 14 will enter the geographical area of the intranet 1. If they are in the middle of a call, their phone will continue to send and receive signals via the external BTS to which it is already connected, thus using the external network as normal. At the end of the call, or if they enter the intranet area whilst not in the middle of a call, their phone will automatically try to attach to the BTS 3, since this would be the closest one.

[0040] This attempt to attach is called a Location Update (LU) request. The intranet BTS 3 is similar to normal external BTSs, hence mobile phones will try to attach to it as they would any BTS which comes into geographical proximity.

[0041] The method of operation of the system is shown in figure 2.

[0042] Upon receiving an LU, the BTS 3 sends the signal to the IMC 4. When the IMC 4 receives the signal, it accesses the MTS for information as to whether the user is to be allowed to access the network. The MTS checks the ILR database 6. This ILR contains a list of all the company members' IMSIs, or has other identifier information such as phone numbers that allow members belonging to the company network to be identified. This identifier is preferably the same as is used in the LU request message, to allow matching to be done easily. The ILR sends a signal back to the MTS indicating whether the LU request is from a company member or a visitor.

[0043] If the signal received back by the MTS indicates that the LU is from a company member, it informs the IMC as such and the IMC then allows the phone to attach to the BTS 3. This means that internal calls be-

tween two employees are routed from the first employee to a BTS 3, to the IMC 4, to the MTS 5 and to the second employee via the BTS 3. External calls from an employee to any phone outside the intranet are routed via BTS 3, to the IMC 4, to the MTS 5 and to the A-Intranet Gateway 7, where they are transferred over the A-interface to the TCSM 11. From here they are sent to the MSC and then forwarded to the BSC 12 and to a BTS 13, from where the phone can receive them.

[0044] If the signal received back by the MTS indicates that the LU is from a visitor, the MTS makes a decision as to whether to allow the visitor to access the intranet. This is possible because it can be configured in two ways by use of a single parameter. The parameter can be set by the company IT department, to allow or reject the LU request. The advantage of this process is that the IT department can decide at any particular time whether or not to allow visitors access to the intranet. This could be important at busy periods during which visitors cause considerable extra load on the system. Thus a high service quality can be maintained at all times for company members. The GSM operator may also have the ability to set the parameter, to allow load on the external GSM network to be relieved by the RCP network.

[0045] If the parameter is set so as not to allow visitors access to the intranet, the MTS sends an appropriate signal to the IMC which then prevents the BTS 3 from allowing the phone to attach to it. The phone will remain attached to or search for the nearest external BTS. This can be done using standard GSM codes.

[0046] If the parameter is set so as to allow visitors access to the intranet, the MTS sends a different signal to the IMC which allows the BTS to attach to the phone. The visitor's calls are then routed through the LAN and out to the external system. The facility for direct access to other phones within the intranet would not be available to visitors. Nevertheless, the fact that their calls are routed through the intranet would improve the quality of reception for the visitor.

[0047] The parameter does not indicate the ability of specific users to access the intranet. Specific additional users can be allowed access by making additions to the database of members. In a GSM-based system the location update request is not a prerequisite to the making of a handover from one base station to another. Thus the system as described above would not, in such a GSM-based system, deny access to the intranet to terminals that requested handovers into the RCP system.

[0048] Such handovers may be tolerated, or could be blocked (at least to non-member terminals) by other means associated with the handover procedure.

[0049] It is possible that the company intranet would be owned by the external operator and leased by the company. The system would then operate in a similar manner except the ILR would communicate via the PCM interface through the MSC 10 to the VLR 8 and the HLR AC EIR 9 owned by the operator. This means, for exam-

ple, that the ILR would be interrogated to determine whether an LU request was from a RCP member or not. Furthermore the VLR8 could be used to list visitors who were temporarily using the office network 1.

Claims

1. An access control system for controlling access by wireless terminals to a wireless telecommunications network, the access control system comprising:

a database storing the identities of a set of wireless terminals belonging to the telecommunications network; a configurable store for storing a supplementary access value indicative of whether terminals that do not belong to the telecommunications network may access the network; and an access control unit for receiving an access request message indicating the identity of a wireless terminal and in response to that message accessing the database and/or the store to permit access by the wireless terminal to the wireless telecommunications network if:

- a. the identity of the wireless terminal is present in the database; or
- b. the supplementary access value indicates that terminals that do not belong to the telecommunications network may access the network.

2. An access control system as claimed in claim 1, wherein the access control unit is configured to, in order to permit access to the said network, send a reply to the access request message indicating that access to the said network is permitted.

3. An access control system as claimed in claim 2, wherein the access control unit is configured to, if:

- a. the identity of the wireless terminal is not present in the database; and
- b. the supplementary access value indicates that terminals that do not belong to the telecommunications network may not access the said network; send a reply to the access request message indicating that access to the said network is not permitted.

4. An access control system according to any preceding claim, wherein the said network is operable according to the GSM standard or a derivative thereof.

5. An access control system according to any preceding claim, wherein the other wireless telecommuni-

cations network is operable according to the GSM standard or a derivative thereof.

6. An access control system according to claim 4 or 5, as dependant directly or indirectly on claim 3, wherein the said message to the other wireless telecommunications network indicating that access to the said network is not permitted is a location update reject message with location access not allowed.

7. An access control system as claimed in any preceding claim, wherein the said access is a location update access.

8. An access control system as claimed in any preceding claim, wherein the said identities of wireless terminals are IMSIs.

9. An access control system as claimed in any preceding claim, wherein the said telecommunications network is a cellular telephone system.

10. A method for controlling access by wireless terminals to a wireless telecommunications network having a database storing the identities of a set of wireless terminals belonging to the telecommunications network and a configurable store for storing a supplementary access value indicative of whether terminals that do not belong to the telecommunications network may access the network; the method comprising:

receiving an access request message indicating the identity of a wireless terminal; accessing the database to determine whether the identity of the wireless terminal is present in the database and/or accessing the supplementary access value to determine whether it indicates that terminals that do not belong to the telecommunications network may access the network; and if the identity of the wireless terminal is present in the database, or the supplementary access value indicates that terminals that do not belong to the telecommunications network may access the network, transmitting a message to permit the wireless terminal access to the wireless telecommunications network.

FIG.1

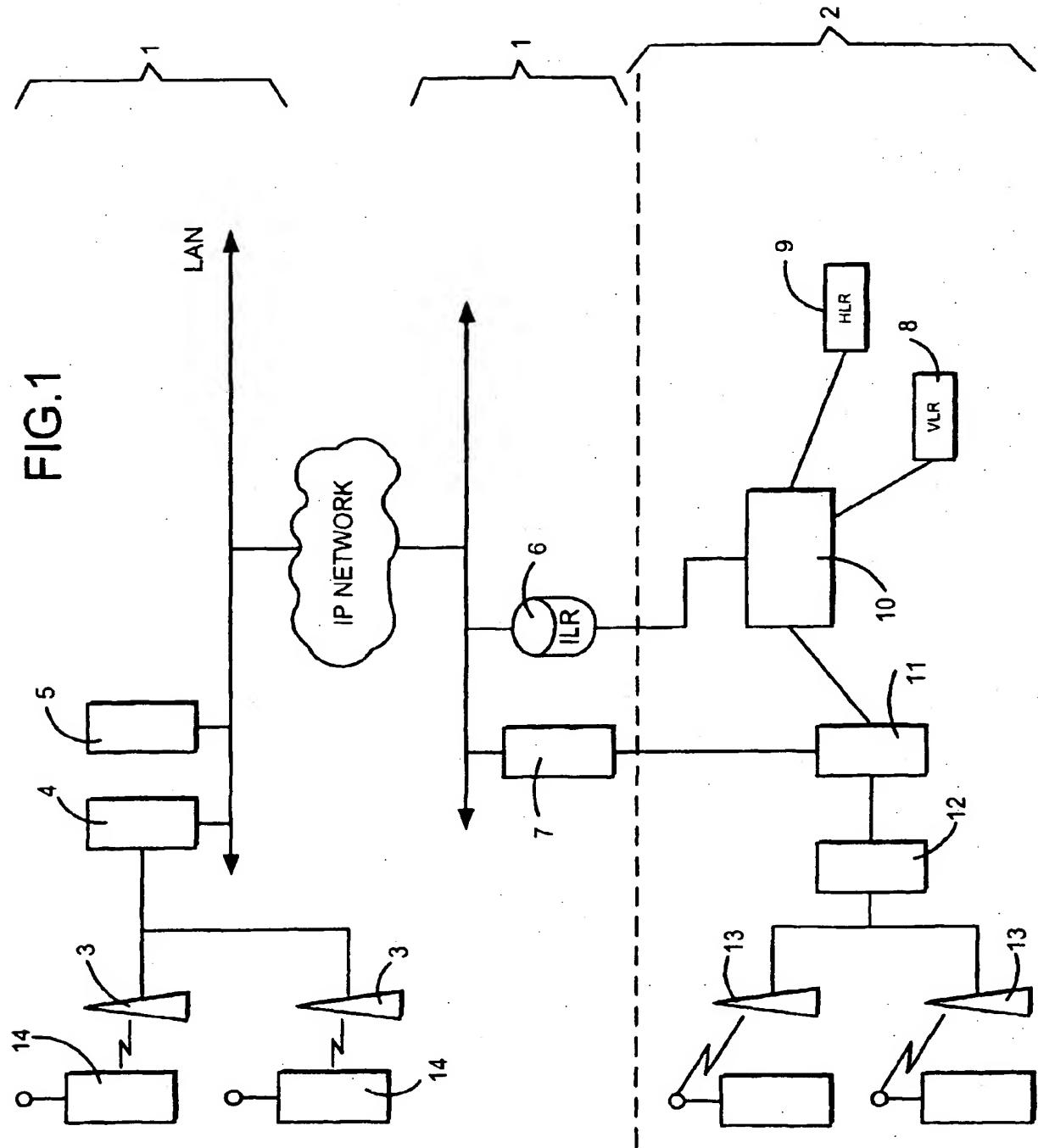
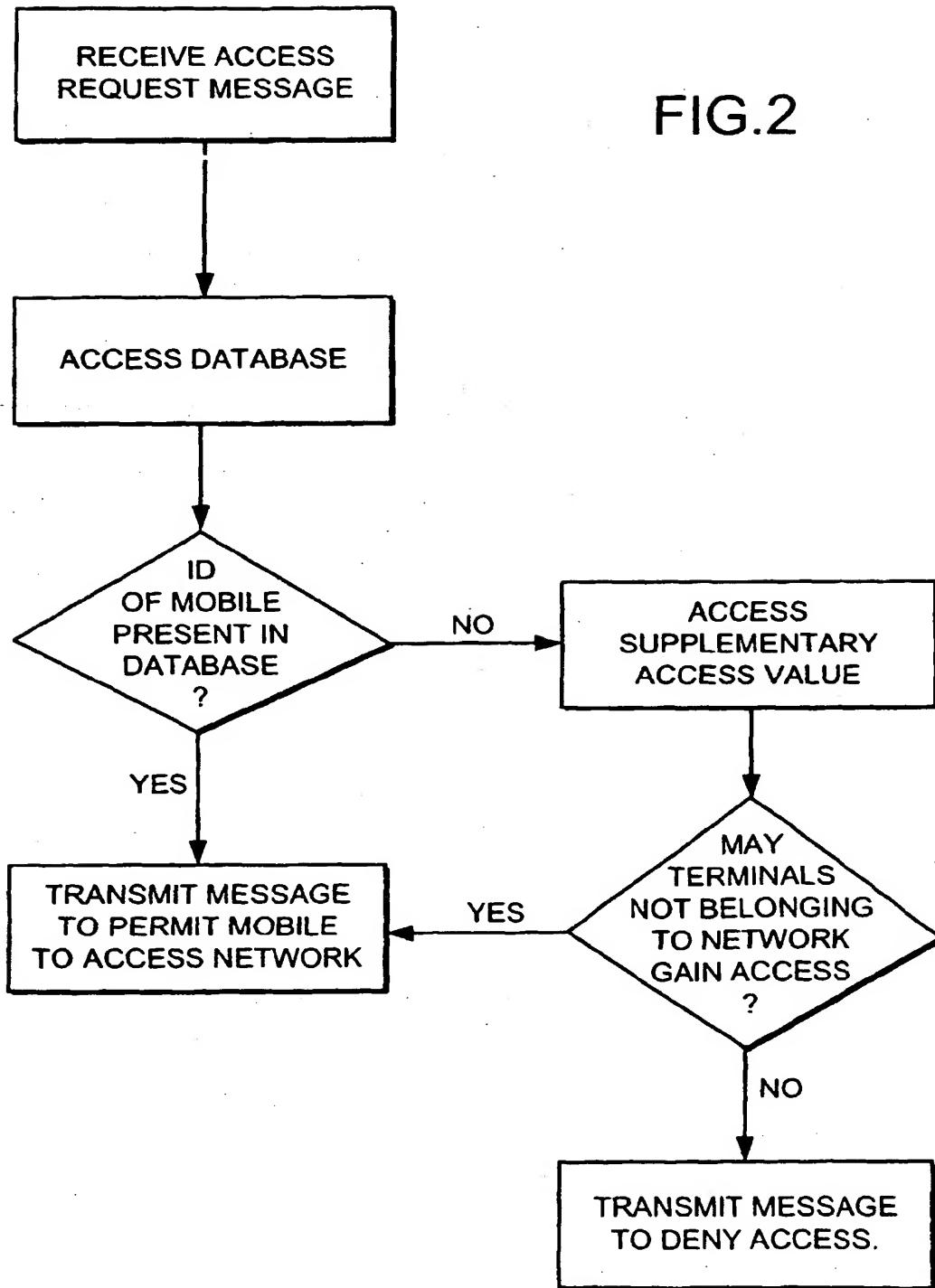


FIG.2





DOCUMENTS CONSIDERED TO BE RELEVANT			CLASSIFICATION OF THE APPLICATION (Int.Cl.)												
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim													
X	US 5 670 950 A (NEC CORPORATION) 23 September 1997 (1997-09-23) * column 2, line 46 - column 7, line 31 *	1,2,4,5, 7-10	H0407/24												
X	WO 97 34437 A (ERICSSON TELEFON AB L M) 18 September 1997 (1997-09-18) * page 3, line 10 - page 5, line 22 * * page 10, line 1 - page 12, line 14 * * page 19, line 8 - page 20, line 2 * * page 24, line 3 - page 25, line 9 * * page 28, line 10 - page 29, line 21 *	1,4,5, 8-10													
A	DE 196 30 399 C (SIEMENS AG) 16 October 1997 (1997-10-16) * column 2, line 17 - column 3, line 51 * * claims 1-13 *	1,10													
A	US 5 793 762 A (PENNERS JOHN HENRY HUBERT ET AL) 11 August 1998 (1998-08-11) * column 2, line 53 - column 4, line 45 *	1,10													
			TECHNICAL FIELDS SEARCHED (Int.Cl.)												
			H04Q												
<p>The present search report has been drawn up for all claims</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Place of search</td> <td style="width: 33%;">Date of completion of the search</td> <td style="width: 34%;">Examiner</td> </tr> <tr> <td>THE HAGUE</td> <td>22 September 2000</td> <td>Kokkoraki, A</td> </tr> <tr> <td colspan="2">CATEGORY OF CITED DOCUMENTS</td> <td></td> </tr> <tr> <td colspan="2"> X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document </td> <td> T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document </td> </tr> </table>				Place of search	Date of completion of the search	Examiner	THE HAGUE	22 September 2000	Kokkoraki, A	CATEGORY OF CITED DOCUMENTS			X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document
Place of search	Date of completion of the search	Examiner													
THE HAGUE	22 September 2000	Kokkoraki, A													
CATEGORY OF CITED DOCUMENTS															
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document													

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 00 30 6447

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
 The members are as contained in the European Patent Office EDP file on
 The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-09-2000

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
US 5670950	A	23-09-1997		JP 2590739 B JP 8033029 A AU 699320 B AU 2498495 A CA 2153859 A	12-03-1997 02-02-1996 03-12-1998 25-01-1996 14-01-1996
WO 9734437	A	18-09-1997		US 5890064 A AU 711632 B AU 2049097 A CA 2247979 A CN 1217861 A EP 0886984 A JP 2000506694 T	30-03-1999 21-10-1999 01-10-1997 18-09-1997 26-05-1999 30-12-1998 30-05-2000
DE 19630399	C	16-10-1997		CN 1226365 A WO 9805178 A EP 0914748 A JP 3068207 B JP 11514187 T	18-08-1999 05-02-1998 12-05-1999 24-07-2000 30-11-1999
US 5793762	A	11-08-1998		US 5457736 A	10-10-1995